

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Description

BUSINESS METHOD FOR SECURE DOCUMENT FOLDER DISTRIBUTION

Inventors: Roger D. Melen, Boris Krtolica, Neil Williams

Background of The Invention

1. Field of the Invention

This invention relates generally to distribution of collections of large documents in electronic form, and more particularly, to a business method for secure document folder distribution.

2. Description of Background Art

The expanded popularity of the Internet has brought new problems to Internet users. As users conduct more business over the Internet, they need to send collections of large documents. Electronic mail has become a popular and widespread means for communicating electronically via interlinked computers. Files, including electronic image files, may be attached to electronic mail messages. Small documents may be sent easily through the Internet as file attachments. Larger documents and collections of larger

1 documents of more than 5 MB, however, are more difficult to
2 send reliably through the Internet without losing the
3 benefit of security.
4

5 Furthermore, sending collections of large documents of
6 more than 5 MB over the Internet is very time-consuming and
7 takes up a lot of network resources. For example, if a
8 sender wants to transmit the same document to ten
9 recipients, he needs to attach ten electronic image files
10 to electronic mail messages, thereby significantly
11 increasing the delivery time.
12

13 What is needed, therefore, is a method and system
14 that allows a sender to send collections of large documents
15 to possibly multiple recipients in a short period of time.
16

17 Disclosure of Invention

18

19
20 The present invention is a system, method, and
21 computer readable medium for a business to securely
22 distribute document folders (180) to recipients (140). The
23 system comprises a sending device (160) for sending the
24 document folders (180) and temporarily storing the document
25 folders (180) on a network (120) of interconnected
26 computers (170), a destination computer (170) for
27 accumulating the sent document folders (180) stored on the
28

1 network (120), and a receiving device (130) for receiving
2 the sent document folders (180) from the destination
3 computer (170).
4

5 The method comprises the steps of sending the document
6 folders (180) to a network (120) of interconnected
7 computers (170); notifying each recipient (140) of the sent
8 document folders by means of an indirect reference to the
9 electronic document folders (180); selecting a destination
10 location (170) for the electronic document folders using
11 data supplied by each recipient (140); and accumulating the
12 electronic document folders (180) at the destination
13 location (170).
14

15 An advantage of the present invention is that it
16 allows distributing collections of large documents of more
17 than 5 MB to multiple recipients (140) in a short period of
18 time without overly consuming network (120) resources.
19

20 Brief Description of the Drawings

21
22
23 The above and other more detailed and specific objects
24 and features of the present invention are more fully
25 disclosed in the following specification, reference being
26 had to the accompanying drawings, in which:
27
28

1 Figure 1 is a block diagram of a preferred embodiment
2 of the present invention.
3

4 Figure 2 is flow chart illustrating a preferred
5 embodiment of the present invention.

6 Figure 2A illustrates an example of a database record
7 222 provided by a recipient 140 to retrieve an electronic
8 document folder 180.

9 Figure 3 illustrates a block diagram of a seal 302
10 attachment system usable in the present invention.
11

12 Figure 4 is a block diagram illustrating an
13 administrative subsystem 410, a billing subsystem 420, and
14 a billing database 430 located on a server 170 of the
15 present invention.

16 Figure 5 is a block diagram illustrating billing
17 database 430.

18 Figure 6 is a block diagram showing an example of a
19 billing record 510.
20

21 Figure 7 is a flow chart illustrating an operation of
22 billing subsystem 420.

23 Figure 8 is a flow chart illustrating an operation of
24 administrative subsystem 410.

25 Figure 9 shows an overview of a client registration
26 process according to a preferred embodiment of the present
27 invention.
28

1
2
3
4 Detailed Description of the Preferred Embodiments
5

6 The present invention is a system, method, and
7 computer readable medium for a business to securely
8 distribute document folders 180 to recipients 140.
9

10 The configuration depicted in Fig. 1 includes at least
11 one, and preferably a plurality of, senders 110; at least
12 one document folder 180 that sender 110 wants to send to at
13 least one recipient 140; a sending device 160; document
14 folders in electronic form 190; a network 120 of
15 interconnected computers 170; at least one destination
16 computer 170; at least one receiving device 130 associated
17 with each destination computer 170; an optional
18 notification device 135; one or more recipients 140; and an
19 optional seal engine 150. More than one recipient 140 can
20 be associated with each receiving device 130. Each
21 document folder 180 contains at least one, and typically a
22 plurality of, documents 178.
23

24 A sender 110 is a person who wishes to send a document
25 folder 180 to one or more recipients 140. Sender 110
26 inputs the document folders 180, which may be in paper or
27 electronic form, into a sending device 160. The sending
28

1 device 160 can be a scanner, a Web-enabled personal
2 computer, a facsimile machine, or any other device which
3 can process documents 178 and output them in electronic
4 form 190. The electronic document folders 190 are sent to
5 the network 120, where they are temporarily stored.
6

7 The purpose of the network 120 is to distribute and
8 process the documents 178. Sending the document folders 180
9 to network 120 avoids a single point of failure. In the
10 event any particular computer 170 in the network 120 fails,
11 the continuous operation of the overall network 120 is not
12 compromised; the network 120 is tolerant to software and
13 hardware problems or faults. Each interconnected computer
14 170 in the network 120 is typically a server computer,
15 including a processor and a memory. The memory includes
16 instructions capable of being executed by the processor to
17 perform the functions described below. Each server 170 can
18 also include a computer readable medium for storing these
19 instructions.
20
21

22 One server 170, e.g., the server 170 shown on Fig. 1
23 as containing database 175, may be entrusted with certain
24 supervisory functions. This computer 170 notifies
25 recipients 140 of document folder 180 delivery. This
26 server 170 optionally records an acknowledgment of document
27 folder 180 delivery and makes said acknowledgment available
28

1 to sender 110. One or more servers 170 may also process
2 sent document folders 180 to convert them into a different
3 format or formats (such as a page description language) to
4 assure they work optimally with each receiving device 130;
5 perform an optional authentication process; and/or perform
6 administrative and billing functions.
7

8 One or more computers 170 accumulate sent document
9 folders 180 for delivery to recipients 140. These
10 computers 170 are known as destination computers 170 or
11 destination locations 170. More than one recipient 140 can
12 select the same destination computer 170. Conversely, each
13 recipient may retrieve document folders 180 from more than
14 one destination computer 170. Each destination computer
15 170, which can be any server 170 in the network 120, is
16 preferably located at a partnership business facility that
17 has agreed to participate in the business of securely
18 distributing document folders 180 to recipients 140. The
19 partnership business facility can be any facility providing
20 printing or photocopying services to clients (e.g.,
21 Kinko's).

22
23
24 When a recipient 140 wishes to retrieve electronic
25 document folders 180, the recipient 140 provides to the
26 notifying server 170 information from the indirect
27 reference to the electronic document folders 180 that was
28

1
2 contained in the notification to the recipient 140, and
3 possibly other data 222. This data 222 supplied by
4 recipient 140 is recorded in database 175, which is located
5 on at least one of the servers 170.

6 At least one receiving device 130 is associated with
7 each destination computer 170, preferably co-located at the
8 same partnership business facility. Receiving device 130
9 can be a Web-enabled personal computer; a Web-enabled
10 printer, such as kiosk printer, connected to network 120; a
11 Web-connected digital copier that has a built-in personal
12 computer with Internet connection; or an Internet
13 appliance, which could be a Web-enabled television.

14
15 The system further optionally includes one or more
16 separate notification devices 135 to assist recipient 140
17 in receiving notifications of sent electronic document
18 folders 180. Alternatively, notification of sent documents
19 178 can be made through a destination computer 170 and/or a
20 receiving device 130. Notification device 135 can be a
21 Web-enabled personal computer, a Web-enabled Internet
22 appliance, a cellular telephone, or any other device
23 capable of sending messages to recipients 140. Receiving
24 notification via notification device 135 advantageously
25 gives recipients 140 timely knowledge of when a sender 110
26 has sent document folders 180.
27
28

Optional seal engine 150 is co-located with at least one computer 170. Engine 150, which may be embodied in hardware, firmware, and/or software, encodes information and attaches a seal 302 to documents 178 based upon instructions conveyed from senders 110 and/or recipients 140. Seal engine 150 is used for authentication purposes to assure that a document 178 which apparently came from a sender 110 is a document actually sent by the sender 110. The seal 302 is a digital collection of information which may be encoded into the image 190 of the document 178. The information contained in seal 302 provides surety and guards against forgery.

The system is described above in connection with the Internet as network 120. However, a wide variety of networks 120, including local area networks (LANs), wide-area networks (WANs), and intranets can be used instead.

Figure 2 illustrates that the method of the present invention starts 200 by a sender 110 sending one or more document folders 180 to the network 120, at step 203. The sender 110 typically forwards the document folders 180 to sending device 160. In one embodiment of the present invention, the sender 110 scans the document folders into a scanner 160 (or the sender instructs the business to scan the document folders into the scanner 160 for him). In an

1 alternative embodiment, the sender 110 forwards the
2 documents 178 to the network 120 from his personal computer
3 160. Device 160 typically converts the documents 178 into
4 images 190. Information in the document folders 180 is
5 distributed, e.g., by being broken up into packets, into
6 the network 120, where it is temporarily stored.
7

8 The clients of the business (anyone from the group of
9 senders 110 and recipients 140) have an option of
10 specifying a date of expiration of the document folders 180
11 stored on the network 120. Also, the business and one or
12 more clients 110, 140 can mutually agree upon the period of
13 time the document folders 180 can be stored on the network
14 120 at no cost to the client 110, 140. It should be noted
15 that a given document folder 180 might comprise only one
16 document 178 or a plurality of documents 178. The
17 documents 178 can be in different file formats, such as
18 audio, video, or formats having printable representation.
19 One of the best modes of carrying out the present invention
20 is sending documents 178 having printable representation,
21 so that remote recipients 140 can conveniently print the
22 sent documents 178 at a convenient destination location
23 170.
24

25 The document folders 180 can be sent to the network
26 120 using virtual private network (VPN) security. A VPN is
27
28

1 a network that is constructed using public wires to connect
2 nodes. There are a number of VPN systems that enable one to
3 create networks using the Internet as the medium for
4 transporting data. These systems use encryption and other
5 security mechanisms to ensure that only authorized users
6 can access the network 120 and that the data cannot be
7 intercepted.
8

9 Once the document folders 180 have been temporarily
10 stored on the network 120, the documents 178 are typically
11 converted into a page description language or format 190
12 (in step 204 of Fig. 2) by one of the computers 170.
13 Converting a document 178 into page description format
14 (PDF) does not allow a recipient 140 to change the format
15 and content of the received document 178. This feature
16 provides for portability and commonality of format and can
17 mask some anomalies of technology on the reception end.
18 PDF captures formatting information from a variety of
19 desktop publishing applications, making it possible to send
20 formatted documents and have them appear on the recipient's
21 monitor or printer 130 as the sender 110 intended them.
22 Alternatively, conversion to PDF can be done by sending
23 device 160 prior to transmitting the documents 180 onto the
24 network 120.
25
26
27
28

1 In step 205, one of the computers 170 notifies
2 recipient 140 of a sent document folder 180 by means of
3 providing an indirect reference to the document folder 180.
4 An indirect reference to the electronic document folder 180
5 can be a folder code containing information needed to
6 retrieve the document folder 180. This information can be,
7 for example, a document number.

9 A folder code may be a privacy code or mediacard data.
10 A privacy code can be automatically sent to recipient 140
11 via e-mail when the document 178 is available for access
12 from the network 120. This privacy code may be a simple
13 set of numbers and may be viewed on a simple display 130,
14 135, such as found on many cellular phones. The privacy
15 code, which arrives in an encrypted form, helps to ensure
16 that unauthorized users cannot access the sent document
17 folders 180. To read an encrypted file, recipient 140 must
18 have access to a password that enables recipient 140 to
19 decrypt it. The encryption and decryption can be performed
20 using symmetric key (secret key) or asymmetric key (public
21 key) cryptography.

24 When public key cryptography is used, two keys are
25 used--a public key known to everyone and a private or
26 secret key known only to the recipient 140 of the message.
27 When a sender 110 wants to send a secure document to a
28

1 recipient 140, the sender 110 uses the recipient's public
2 key to encrypt the message. Recipient 140 then uses his or
3 her private key to decrypt it. At least one server 170
4 located on the network 120 has a table of clients' names
5 and their corresponding public keys. When the designated
6 server 170 sends a notification message to a recipient 140,
7 recipient 140 can decrypt the message using his or her
8 private key.

10 A folder code can also be mediocard data. A mediocard
11 is an electronic device that contains electronic memory. A
12 mediocard preferably should be delivered to a recipient 140
13 prior to document folder 180 retrieval. Such a mediocard
14 may be created using a networked transmission of mediocard
15 data as part of the mediocard delivery process.

17 It should be noted that the document folder 180
18 retrieval need not be based on privacy code or mediocard
19 data. Any data providing an indirect reference to
20 electronic document folders 180 can be used in the delivery
21 process.

23 The indirect reference notification can arrive at
24 notification device 135 or receiving device 130. The
25 notification can be in the form of e-mail if device 135 is
26 a Web-enabled personal computer, or via voice mail if
27 device 135 is a cellular telephone, or by a combination of
28

1 e-mail and voice mail. The notification message informs
2 recipient 140 that at least one document folder 180 has
3 been sent to that recipient 140 and is ready for pickup.
4

5 Once the notification arrives at device 135, a
6 designated computer 170 selects a destination location or
7 locations 170 for the electronic document folders 180 using
8 data provided by each recipient 140, in step 206. Such
9 data can include document 178 reception address data,
10 and/or additional document 178 reception data.
11

12 Document 178 reception address data can be path
13 information and/or method for network document folder 180
14 delivery. An example of document 178 reception address
15 data is:

16 ftp:/avistadel.com/doc/print/tty.prn (see Fig. 2A)

17 Additional document 178 reception data can include
18 document 178 reception location data (data used for
19 improving the document 178 delivery experience through the
20 knowledge of the geographical location of the receiving
21 equipment 130 and the destination location 170 of the
22 receiving equipment 130) and/or receiving device 130
23 capabilities (screen/printer capabilities of the receiving
24 device 130, such as text/graphics, color or black and white
25 representation).
26
27
28

1 In step 207, the process proceeds by a designated
2 computer 170 optionally automatically modifying information
3 contained in document folders 180 for best recipient 140
4 use with regard to receiving device 130 capabilities. For
5 example, if the receiving device 130 is a black and white
6 printer, the business may have decided that it is desirable
7 to modify document 178 data to remove any color information
8 contained in document images 190 for fastest transmission
9 on the network 120. Similarly, if the receiving equipment
10 130 has text, but not graphic capabilities, the business
11 may have decided that it is desirable to modify the
12 document 178 data so that only text is included.

13
14
15 Recipient 140 or sender 110 may optionally (in step
16 208) request authentication of documents 178 to assure that
17 recipient 140 takes delivery of an actual document 178 sent
18 by sender 110, and not a forged document. When the
19 authentication process is included, seal 302 is attached to
20 a document 178 by seal engine 150. The seal 302 is a
21 digital collection of information which may be encoded into
22 document image 190.

23
24 In step 210, a designated computer 170 causes the sent
25 document folders 180 to accumulate on destination computer
26 170 using data 222 provided by recipient 140. When
27 recipient 140 requests the designated computer 170 to
28

1 deliver the sent document folders 180, he or she may select
2 the destination computer 170 to be used.

3
4 To retrieve the sent document folders 180, recipient
5 140 is prompted in step 212 by the designated computer 170
6 to enter information from the indirect reference
7 notification. For example, this information may be a
8 document number. The business may impose a requirement
9 that recipient 140 provide this information in encrypted
10 form.

11
12 In step 214, recipient 140 takes document delivery
13 based on all the information and data 222 submitted, using
14 receiving device 130.

15 Once recipient 140 takes delivery of document folders
16 180, the process ends in step 216.

17 Figure 2A illustrates an example of typical data 222
18 provided by recipient 140 to optimize and tailor the
19 retrieval of electronic document folders 180. This data
20 222 supplied by recipient 140 is sent to database 175,
21 which is located on at least one of the servers 170. An
22 exemplary data record 222 has the following fields:
23 sender's name, recipient's name, document 178 reception
24 address data, and additional document 178 reception data.
25 The latter field is broken into two subfields: receiving
26
27
28

1 device 130 capabilities and document 178 reception location
2 data.

3
4 The document 178 reception address data can include
5 path information and/or method for network document folder
6 180 delivery.

7 The document 178 reception location 170 data is
8 particularly useful when the document 178 may be sent to
9 several destination servers 170 throughout the world. The
10 document 178 reception location 170 data is used for
11 improving the document 178 delivery experience by using the
12 geographical location of the receiving device 130 and the
13 network 120 location of the receiving device 130. The
14 preferred destination server 170 for document 178 delivery
15 may be determined using this location data.

16
17 Recipient 140, using notification device 135 and/or
18 receiving device 130, is prompted in step 212 to provide
19 any document 178 reception address data and any additional
20 document 178 reception data before the destination location
21 170 is selected for the document folders 180 delivery.
22 This data 222 is recorded in database 175. The exemplary
23 database record 222 shown in Fig. 2A includes a sender's
24 name= "SMITH"; a recipient's name="WARREN"; document 178
25 reception address data=
26
27 "ftp://avistadel.com/doc/print/tty.prn; receiving device 130
28

capabilities= "color, 300dpi, pdf"; document 178 reception location data = 73 DX STREET, BESTTOWN, CA 59959, and the Internet address of the nearest server 170 to the receiving location 130: 333.444.555.66. Once recipient 140 provides the above data 222, the designated computer 170 (typically computer 170 co-located with database 175) selects the destination location 170 for the document folder 180 delivery. Some or all of the data 222 can be provided to the designated supervisory computer 170 automatically by receiving device 130. Alternatively, data 222 can be hand-entered into receiving device 130 or notification device 135, by recipient 140.

Figure 3 is a block diagram of a seal 302 attachment system. When the authentication step 208 is included, seal 302 is attached to the document 178 by seal engine 150. The seal 302 is a digital collection of information which may be encoded into a document image 190. In one embodiment of the present invention, the attached seal 302 includes information contained in the sent document 178, such as a portion of image 190 of the sent document 178, as well as information not contained in the sent document 178, which information might include one or more pieces of key information, such as a file size, a date and time of transmission, a protocol identification, such as

1 Transmission Control Protocol/Internet Protocol (TCP/IP),
2 and information known only by a recipient 140, such as the
3 recipient's mother's maiden name.
4

5 In the illustrated example, sender 110 wants to send a
6 title transfer document 300 to a recipient 140. As a
7 result of the authentication procedure, seal engine 150
8 attaches seal 302, encoding a complete representation of
9 the original document 178 as well as information not
10 contained in the sent title transfer document 300. Such
11 information includes the following: a file size of 7 MB, a
12 date of transmission 8/24/00, a time of transmission 3:24
13 P.M. Pacific Daylight Savings Time, protocol information
14 TCP/IP, and "Watson" as the recipient's mother's maiden
15 name. The latter information is useful for authentication
16 because only an intended recipient 140 is likely to know
17 this information. The printed title transfer document 304
18 that is sent to recipient 140 has the attached seal 302.
19 The seal 302 embodiment of the present invention
20 advantageously allows assuring that the received document
21 178 is an authentic one.
22
23

24 Fig. 4 is a block diagram illustrating an
25 administrative subsystem 410, a billing subsystem 420, and
26 a billing database 430 that are typically located on at
27 least one server 170 (for example, the server 170 co-
28

located with database 175). It should be understood that the architecture shown in Fig. 4 is an example only and is not to be construed in a limiting sense.

A sender 110 may periodically deliver document folders 180 to the same group of recipients 140. As such, it is advantageous for the business to register clients 110, 140 and keep client 110, 140 accounts in one database 430. The administrative subsystem 410 is a system for registering clients 110, 140 and managing system resources based on client 110, 140 requests. The administrative subsystem 410 communicates with billing subsystem 420. The billing subsystem 420 detects monetizing (billing) events generated by the administrative subsystem 410. The billing subsystem 420 can be programmed to charge clients 110, 140 differently for different monetizing events, such as a recipient 140 taking delivery of document folders 180 when the document folders 180 are sent C.O.D. (cash on delivery). A client 110, 140 has an option of specifying a date of expiration of the document folders 180 temporarily stored on network 120. The billing subsystem 420 then charges clients 110, 140 when the document folders 180 are stored beyond the period of time agreed upon by the business and the client 110, 140. The billing subsystem 420, in turn, communicates with billing database 430, which

1 may be part of database 175 or a separate database.

2 Billing database 430 maintains and adjusts client 110, 140
3 accounts based on information received from billing
4 subsystem 420. Once a monetizing event occurs, that
5 information along with a client 110, 140 name is submitted
6 to billing database 430 to adjust the account of the client
7 110, 140.
8

9 Figure 5 is a block diagram illustrating billing
10 database 430. Billing database 430 contains billing
11 records 510. Each billing record 510 provides billing
12 information about a particular client 110, 140.
13

14 Fig. 6 is a block diagram showing an example of a
15 billing record 510, in which billing record 510 has the
16 following two fields: client 110, 140 name and client 110,
17 140 billing information. The client 110, 140 billing
18 information may include a client 110, 140 account number,
19 the entity to whom the bill is to be sent, and how the
20 client 110, 140 takes responsibility for the payment. When
21 a monetizing event occurs, a memorandum of that event along
22 with the client 110, 140 name is forwarded to the billing
23 database 430, which, in turn adjusts the client 110, 140
24 account.
25

26 Fig. 7 is a flow chart showing the operation of
27 billing subsystem 420. The process starts in step 700. In
28

1 step 702, a periodic query asks whether billing event has
2 taken place. The event could be any monetizing event, such
3 as sending a document folder 180, sending a document folder
4 180 C.O.D, storing a document folder 180 on destination
5 computer 170 beyond the agreed-upon period of time, or
6 requesting transmitting a document folder 180 with
7 authentication so that a seal 320 is attached. Once a
8 monetizing event occurs in step 702, the administrative
9 subsystem 410 sends information regarding the event
10 including the client's name to the billing subsystem 420,
11 in step 704. The billing subsystem 420 forwards all this
12 information to the billing database 430, in step 706. The
13 billing database 430 adjusts the client's account based on
14 the information received from the billing subsystem 420, in
15 step 708. The process ends in step 710. If the
16 determination in step 702 is negative so that no monetizing
17 event has taken place, the process loops to the end 710 and
18 the client's account is not adjusted.

19
20
21
22 Fig. 8 is a flow chart illustrating one operation of
23 administrative subsystem 410. The administrative process
24 includes registering clients 110, 140 and maintaining
25 client 110, 140 resources. In step 802, the process
26 starts. First, a client 110, 140 registers with the
27 business by filling out a registration form in step 804.
28

Filling out the registration form, which may be, for example, a form presented on the World Wide Web, may require providing the client's name, address, and password for authorization purposes. In step 806, an authorization process takes place. Specifically, the business verifies whether a client 110, 140 is who he claims he is. This verification can be accomplished, for example, by sending an e-mail to the client 110, 140 and requesting a response, or by a human being calling the prospective client 110, 140 on the telephone. The process allows the client 110, 140 to submit new client information in step 807, if needed to complete the registration requirements as defined by the business. All the information submitted by the client 110, 140, including the client's name and address, is forwarded in step 808 to the billing database 430. The process ends at step 810.

Fig. 9 shows an overview of a typical client registration process (step 804 described above). In display 902, the client 110, 140 is asked to register with the business. To do so, the client 110, 140 fills out a form, in this case an online form. The client 110, 140 may be prompted by software contained in the administrative subsystem to enter his name and address, and select a password. Further, in display 904, the client is prompted

1 to re-enter his password for authentication purposes. In
2 other embodiments, a non-password based authorization check
3 might be used. The client's password is an important piece
4 of information, which is used during the client 110, 140
5 authentication process to ensure that only clients 110, 140
6 registered with the business can send and receive document
7 folders 180. Once the client 110, 140 provides all
8 identification information, a message is displayed in 905
9 informing the client 110, 140 to submit his registration
10 information, e.g., by clicking on a "submit" button on his
11 computer screen. In display frame 906, the client 110, 140
12 is notified that all of his registration information will
13 be submitted to billing database 430.
14

15
16 The above description is included to illustrate the
17 operation of the preferred embodiments and is not meant to
18 limit the scope of the invention. The scope of the
19 invention is to be limited only by the following claims.
20 From the above discussion, many variations will be apparent
21 to one skilled in the art that would yet be encompassed by
22 the spirit and scope of the present invention.
23

24 What is claimed is:
25
26
27
28